secorvo
security consulting

# Secorvo Security News

**November 2018**

## Ende des Kuschelkurses

Jetzt sind sie da – die ersten DSGVO-Bußgelder. Und tatsächlich: Allen Unkenrufen und wilden Spekulationen zum Trotz, die höchste Bußgelder für Minimalverstöße bei kleinen und mittleren Unternehmen voraussagten, sind sie ein Zeichen von Augenmaß und klarer Kante zugleich.

Während Knuddels nach einem Daten-Leak von Millionen Kundendaten (inklusive Klartext-Passwörtern) als Anerkennung für die unverzügliche Vorfallsmeldung und die enge Kooperation mit der Aufsichtsbehörde bei der Beseitigung der Schwachstellen nur ein moderates Bußgeld in Höhe von 20.000 € auferlegt wurde (siehe den Beitrag in diesen SSN), haben die Aufsichtsbehörden von Großbritannien und den Niederlanden nun den amerikanischen Taxi-Konkurrenten Uber nach einem über ein Jahr geheim gehaltenen Datenschutzvorfall, von dem 57 Millionen Nutzer und Fahrer betroffen waren, mit einem Bußgeld von insgesamt mehr als einer Million Euro belegt.

Die Fälle zeigen dreierlei: So werden gerade aus den zahnlosen Tigern, die die Datenschutzaufsichtsbehörden mit ihren übersichtlichen maximalen Bußgeldern bislang waren, einflussreiche Mitspieler bei der Durchsetzung eines sicherheitssensiblen Umgangs mit personenbezogenen Daten. Dabei konzentrieren sich die Aufsichtsbehörden zweitens, wie von Experten erhofft, mit ihren Bußgeldbescheiden auf tatsächlich materiell relevante Vorfälle – und sanktionieren nicht bürokratische Nachlässigkeit, wie vielfach befürchtet wurde. Und sie senden drittens ein wichtiges Signal in alle Welt: Wer in einem der größten Binnenmärkte Geschäfte mit europäischen Bürgern macht, hat sich an europäisches Datenschutzrecht zu halten – und das gilt, wie der Europäische Gerichtshof schon 2014 deutlich gemacht hat, auch für amerikanische Anbieter. Google, Amazon, Facebook & Co. werden das in Bälde zu spüren bekommen. Womöglich bricht gerade ein neues Datenschutzzeitalter an – „Post Privacy" jedenfalls war gestern.

## Inhalt


**Ende des Kuschelkurses**

**Security News**

Erstes DSGVO-Bußgeld

DSGVO-Services

Autopsy

HeadSetup – Nachlese

Datenschutz-Standardisierung

**Secorvo News**

Teamverstärkung

Seminare

Krypto im Advent

**Veranstaltungshinweise**

**Fundsache**

secorvo
security consulting

# Security News

## Erstes DSGVO-Bußgeld

Bußgelder im Rahmen der DSGVO waren vor Inkrafttreten Zündstoff für hitzige Diskussionen. Es wurde erwartet, dass angesichts des Strafrahmens (maximal 10 bis 20 Mio. € bzw. 2-4% des weltweiten Gesamtumsatzes) hohe, wenn nicht sogar sehr hohe Strafen zur Abschreckung verhängt werden.

Im Fall des Daten-Leaks bei Knuddels, bei dem Millionen Nutzerdaten (inklusive Klartext-Passwörter) abgezogen wurden, wurde nun der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg tätig und verhängte das erste DSGVO-Bußgeld in Höhe von 20.000 € - eine entgegen den Erwartungen moderate Bußgeldhöhe. Doch der Landesdatenschutzbeauftragte begründet die Entscheidung klar und gut nachvollziehbar: Für ihn sei ausschlaggebend, wie sich ein Unternehmen im Falle eines Datenschutzvorfalls verhält. Die Reaktion von Knuddels – umgehende Information aller Betroffenen, zügige Meldung an die Aufsichtsbehörde und Kooperation mit den zuständigen Stellen – sei in dieser Hinsicht vorbildlich gewesen.

Die moderate Höhe des Bußgelds sollte daher nicht als Einladung zu einem nachlässigen Umgang mit Datenschutzbelangen missverstanden werden. Das gilt vor allem, wenn Passwörter und IDs von Nutzern betroffen sind – schließlich handelt es sich dabei um besonders schützenswerte Daten. Daraus folgt vor allem, dass diese sicher gespeichert werden müssen, beispielsweise als Hashwert – jedenfalls unter keinen Umständen im Klartext.

In jüngster Vergangenheit zeigte sich allerdings, dass auch einige andere Plattformbetreiber es mit der Passwortsicherheit nicht so genau nehmen. Mitte des Jahres blamierte sich T-Mobile Österreich auf Twitter, und dann schaffte es Instagram sogar, Passwörter durch ein DSGVO-Tool abfließen zu lassen. Kandidaten für höhere Bußgeldbescheide gibt es also bereits.

## DSGVO-Services

Die Datenschutz-Grundverordnung hat die Benennung des Datenschutzbeauftragten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) neu eingeführt und die Meldung von Datenschutz-Vorfällen (Art. 37 Abs. 7) deutlich aufgewertet, letztere durch eine enge Frist und erhöhte Sanktionen. Einige Aufsichtsbehörden haben die Sanktionierung bei unterbliebener Benennung bis Anfang 2019 ausgesetzt – vielleicht auch, weil für beide Meldeformen nach wie vor nicht alle Online-Meldeportale funktionsbereit sind.

Es fällt auf, dass gerade die großen Bundesländer hier Defizite aufweisen. Während die Online-Benennung außer in Thüringen überall möglich ist, ist eine Online-Vorfallsmeldung (neben Thüringen) auch in Brandenburg, Bremen, Nordrhein-Westfalen, Sachsen und Schleswig-Holstein nicht verfügbar.

Beinahe alle Bundesländer gehen zudem sehr unterschiedliche Wege bei dem Angebot; teilweise sind die Portale sehr versteckt und schlecht zu finden. Hessen bietet den Versand eines Upload-Links für ein ausgefülltes Vorfallsformular an. In Bayern und NRW ist für die Benennung des Datenschutzbeauftragten zudem eine vorherige Registrierung des Verantwortlichen erforderlich. Eine Benennung für mehrere Verantwortliche in einem Online-Formular ist durchweg nicht möglich, entgegen Art. 37 Abs. 2 DSGVO.

Bei der Meldung eines Vorfalls kann durchaus eine fallspezifische Vorlage sinnvoll sein, doch gerade wenn für Unternehmensgruppen die Benennungen vorzunehmen sind, sind die vorhandenen Erschwernisse durchaus ärgerlich – da hinkt die Praxis dem Vereinheitlichungsgedanken der DSGVO noch deutlich hinterher.

## Autopsy

Seit dem 09.11.2018 ist die erheblich verbesserte Version 4.9.1 des kostenfreien forensischen Werkzeugs Autopsy verfügbar und läuft nun bei hoher Last mit vielen Falldaten noch einmal deutlich stabiler. Sehr hilfreich ist die neue Funktion einer zusammengeführten Datenbasis (Central Repository), die validierte und normalisierte Daten fallübergreifend vorhält. Wer bisher dachte, man kann mit Autopsy „nur" Datenträgerforensik durchführen, irrt, denn durch Aktivierung der „Experimental Plugin"-Funktion wird der Zugriff auf den weiterentwickelten Volatility Data Source Processor möglich, so dass Datenträger- und Hauptspeicherartefakte in einer Analyse zusammengeführt werden können.

Beide Funktionen zusammen erlauben eine mächtige Suche nach Gemeinsamkeiten, Querbeziehungen und Datenspuren sowohl für systembezogene als auch systemübergreifende Artefakte. Ein Tool, das in keinem Forensik-Labor fehlen sollte.

## HeadSetup – Nachlese

In den SSN 10/2018 berichteten wir bereits über die Schwachstelle CVE-2018-17612 in Sennheisers HeadSetup. Mittlerweile beschäftigten sich auch

das Microsoft Security Advisory (ADV180029) und diverse weitere Medien mit der Schwachstelle.

Anschließend setzen wir uns mit den möglichen Ursachen dieser Schwachstelle auseinander, denn Katastrophen sind meist das Ergebnis einer Verkettung ungünstiger Ereignisse. So handelt es sich im vorliegenden Fall auch nicht um einen reinen Implementierungsfehler; auch bei Design und Architektur wurden gravierende Fehler begangen – die zur Lösung eines allerdings nicht von Sennheiser zu vertretenden Problems in Kauf genommen wurden.

Denn maßgeblich dafür, dass überhaupt eine CA zur Kommunikation mit dem lokalen Dienst zum Einsatz kam, ist der Umgang der Browser mit sogenanntem Mixed-Content – unverschlüsselten Inhalten, die in mittels HTTPS geschützte Seiten eingebunden werden. Mike West aus dem Chrome Security Team wies schon am 29.04.2016 darauf hin, dass unverschlüsselte Inhalte vom lokalen System als vertrauenswürdig angesehen werden sollten, da ansonsten die Anwender veranlasst werden könnten, neue Root-CAs nur zu diesem Zweck zu installieren. Dies führte Mitte 2016 zu einer Änderung des Standards. Trotzdem unterbindet derzeit ein Großteil der Browser (Firefox 63.0.1, Safari, Internet Explorer 11) genau diese Anfragen. Lediglich Google Chrome und in der aktuellen Version auch Microsoft Edge erlauben die unverschlüsselte Kommunikation mit den lokalen Diensten. Dies führt Entwickler, die lediglich die Kompatibilität ihrer Software mit verschiedenen Browsern gewährleisten wollen, auf dünnes Eis.

Ein „Zuviel" an Sicherheit kann auch Unsicherheit verursachen. Um ähnliche Schwachstellen zukünftig auszuschließen müssen die Browser-Hersteller schnellstens ihre Sicherheitsstrategie den Standards anpassen.

### Datenschutz-Standardisierung

Am 10.09.2018 veröffentlichte das ULD Schleswig-Holstein neue Module des Standarddatenschutzmodells (SDM). Dabei handelt es sich noch um Entwürfe, zu denen nun Anwender ihre Erfahrungen mitteilen sollen. Die vorgestellten Bausteine betreffen die Themen Aufbewahrung, Planung und Spezifikation, Dokumentation, Protokollierung, Trennung, Löschen und Vernichten sowie Datenschutzmanagement. Das SDM soll eine Blaupause für die Prüfung von Verarbeitungstätigkeiten liefern, die gleichzeitig eine Prüfung der Gestaltungsentscheidungen ermöglicht. Die einzelnen Bausteine enthalten unverbindliche Maßnahmenkataloge, die sich am IT-Grundschutz des BSI und den Maßnahmen der früheren Anlage zu § 9 BDSG aF orientieren.

Ob das SDM in der Praxis die versprochene Erleichterung und den Nachvollziehbarkeitsgewinn liefert, hängt von der inhaltlichen Fortentwicklung der Module ab: Noch deckt das Vorgehen nur einen Teil der Verarbeitungstätigkeitsprüfung ab, die Prüfung der Rechtsgrundlage bleibt bspw. außen vor. Das Vorgehen und die Ausführungen zu den Gewährleistungszielen stellen sich recht kompliziert dar und erfordern erhebliche Datenschutzerfahrung zur Einordnung. Den betrieblichen Datenschutzbeauftragten in Nebentätigkeit dürfte dies überfordern.

## Secorvo News

### Teamverstärkung

Auch mit Blick auf die große Nachfrage nach unseren Penetrationstests freuen wir uns sehr, dass seit Mitte November Christian Titze unser Team verstärkt. Und Monika Contag hat das Rechnungswesen übernommen. Willkommen im Team!

### Seminare

Wer seine Weiterbildung 2019 langfristig plant, findet das Seminarangebot, die Termine unserer PKI-, T.I.S.P.- und T.P.S.S.E.-Seminare (alle ab März 2019) sowie die Online-Anmeldung unter www.secorvo.de/seminare.

### Krypto im Advent

Am 01.12.2018 startet unser viertes Adventsrätsel „Krypto im Advent" für Schülerinnen und Schüler der Klassen 3 bis 9. Der in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelte interaktive Adventskalender entführt in die Welt der Kryptologie. Diesmal gilt es, die entführte Geheimagentin Kryptina wiederzufinden.

Wer alle Rätsel richtig beantwortet, kann einen der zahlreichen von unseren Sponsoren beigesteuerten Preise gewinnen. Auch ältere, an der Kryptologie Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

## Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

| | |
|---|---|
| **Dezember 2018** | |
| 03.-06.12. | Black Hat Europe 2018 (Blackhat, London/UK) |
| 27.-30.12. | 35C3 – 35. Chaos Communication Congress 2018 (Messe Leipzig, Leipzig) |
| **Januar 2019** | |
| 18.-20.01. | ShmooCon 2019 (The Shmoo Group, Washington/US) |
| 21.-23.01. | Omnisecure 2019 (in TIME berlin, Berlin) |
| **Februar 2019** | |
| 06.-07.02. | 26. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg) |
| 20.-21.02. | 29. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt) |
| **März 2019** | |
| 18.-21.03. | PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe) |
| 20.-21.02. | T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe) |

## Fundsache

Der Beuth Verlag hat das Taschenbuch 408 zum Informationssicherheitsmanagement herausgegeben. Es enthält acht Normen aus der ISO270xx-Familie sowie die DIN 66398 und ist mit € 180 sogar günstiger als je zwei der enthaltenen Normen zum Einzelpreis. Ein Weihnachts-Schnäppchen...


## Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Dr. Volker Hammer, Michael Knopp, Friederike Schellhas-Mende, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de